计算机网络反病毒解决方案

于泠,陈波

(南京师范大学数学与计算机科学学院,南京,210097)

[摘要] 提出了在不同服务器操作系统的网络环境下反病毒的基本方法,阐述了网络系统整体反病毒措施,并以一个典型的企业级局域网为例,介绍了病毒防护的具体设置方案.

[关键词] 网络安全;计算机病毒;局域网

[中图分类号]TP309.5; [文献标识码]A; [文章编号]1001-4616(2001)02-0026-05

0 引言

随着 Internet 的深入普及以及大规模企业级内部网络的应用,企业级和个人用户对网络的安全越来越感到担忧,网络黑客的攻击等安全性问题已引起人们的重视.实际上许多网络安全问题是由广为传播的计算机病毒造成的.

随着网络的不断扩展,文件服务器、备份服务器、Internet 网关和网络管理系统的增加以及客户机的激增,病毒防御成为一项复杂和困难的工作.对于拥有多种操作系统,采用分布式或客户机/服务器式,通过网络共享、电子邮件和 Internet 进行数据文件自由交换的网络系统,要求反病毒解决方案包括一套统一全面的实施方法.本文对此进行了设计和论述.

1 网络病毒的传播途径

网络病毒的传播途径有 3 个.

通过电子邮件传播.随着 Internet 的迅速发展,将病毒附加在电子邮件中使得病毒的扩散速度急骤提高,受感染的范围也越来越广.

通过工作站传播.这是病毒入侵网络系统最为常见的传播途径.工作站是网络的大门,如果网络上的工作站已感染了病毒,则服务器很快就会被病毒感染.

通过服务器传播.服务器是网络的核心,一旦服务器被病毒传染,服务器无法启动,整个网络就会陷于瘫痪.例如服务器上的 DOS 分区感染了病毒,那么在执行 Server 启动服务器时,病毒就会立即感染 Server.exe,从而使服务器上的文件被病毒感染,这样,即使工作站是干净的,在登录服务后也会被病毒感染.

网络病毒的特点和危害主要是:破坏性大、针对性强.此外,由于病毒的传染性,使得网络病毒的扩散面很广,一台工作站上的病毒可以通过网络通讯线路广为扩散.由于网络规模大,对整个网络进行查毒、解毒比单机的查毒、解毒复杂、繁重得多.

收稿日期:2000-10-09

作者简介:于泠,1972—,女,南京师范大学数学与计算机科学学院硕士研究生,从事计算机信息网络安全系统的学习与研究.

2 混合环境下的网络反病毒

考虑一个使用不同服务器操作系统的混合环境,见图 1.

2.1 客户端反病毒[1]

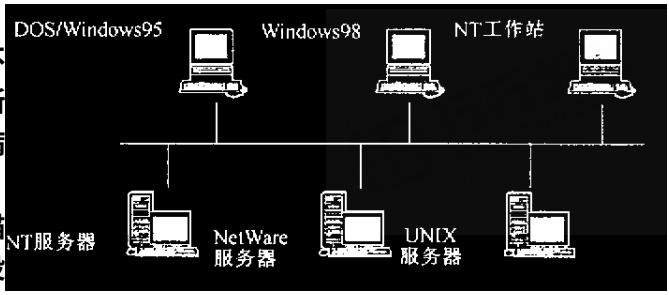

图 1 不同服务器操作系统的混合环境

虽然客户端使用的操作系统不同,但硬件平台基本相同.这意味着所有客户端系统会遭受许多同种类型病毒的攻击.

对所有本地驱动器使用病毒扫描程序定期进行完整的扫描,以确认没有病毒在系统中.在系统初始化时启动内存驻留扫描程序,以在病毒保存到本地文件之前或进入内存运行之前清除.为了减少该扫描程序对系统性能的影响,可以只检查最近经常被感染的文件.内存驻留程序应该重点检查 :只读文件、COM 和 EXE 等可执行文件、具有宏功能的文档.良好的按需扫描程序都应具有启发式扫描能力,还可以把所有扫描过程的结果报告到一个集中的地方,供系统管理员查看.

2.2 NT 和 NetWare 服务器反病毒

由于 NT 和 NetWare 服务器系统是共享资源,因此与客户端机相比它的反病毒显得更为重要,一方面它们自身会感染上病毒,另一方面它们可能成为向客户端系统传播病毒的集散地.

对所有本地驱动器使用病毒扫描程序定期进行完整的扫描,以确认没有病毒在系统中.扫描过程应该在文件系统进行备份之前进行.

使用内存驻留型扫描程序.为 Windows NT 设计的内存驻留型软件会检查服务器的内存以及本地系统中存储的文件.内存驻留型扫描工作在 NetWare 服务器上操作的方式稍有不同,这是因为此种服务器无法运行标准的可执行程序.由于系统只是简单的使用文件存储,所以不必检查内存,最需要注意的是传入网络的信息.基于服务器的内存驻留型扫描程序应该重点检查以下内容 :本地内存中是否有蠕虫程序和特洛伊木马程序 ;进入网络的可执行文件 ;进入网络的具有宏功能的文档.

由于管理员对所有的目录均有写权限,所以当以管理员身份注册时,一定要确信内存中没有驻留病毒.当没有把握时,要以一个对可执行文件存储的目录不具有写权限的用户身份注册.如果可执行文件和数据必须存储于同一目录(用户在此目录中有写权限)时,可以通过设置文件属性为只读属性来预防病毒的攻击.对于从一台或多台服务器上启动的应用程序,设置文件只读属性可以保证可执行文件不被病毒感染.如果所有应用程序都存储在本地工作站上,则服务器上的可执行文件不一定需要设置为用户级只读访问权.

2.3 UNIX 反病毒

侵入 UNIX 系统的病毒较少,用户最需要注意的应该是特洛伊木马程序和蠕虫程序.通常来说,UNIX 系统的反病毒可以从以下三方面考虑.

(1)若 Telnet 服务器程序被替换成攻击者自己生成的程序,它会记录下每个在系统上登录的用户的授权检查信息.我们查找这种威胁性行为的简易方法是进行定期的文件完整性检查.用户还需要检查所有接受入站连接的进程,这些检查过程应该以自动处理的方式运行,并且在

不同机器上对结果进行分析,这样用户可以避免进行结果分析的机器正好是被入侵的机器.

(2)进程监视应该对每个独立系统的结果进行自动的审核和分析,当发现有新进程时用户可以采取相应措施.如蠕虫程序侵入系统会表现为进程显示中出现一个新进程.

(3)缺省状态下,只有超级用户可以覆盖系统中作为服务器运行的软件.普通用户不应该具有对这些文件的写权限,对文件权限的限制可以尽可能地减少系统被入侵的机会.

3　网络反病毒解决方案

3.1　网络病毒预防[2]

网络病毒的预防措施主要有:

(1)除非必要,尽可能地拆除工作站上的软盘驱动器,采用无盘工作站代替有盘工作站,这样能减少网络感染病毒的机会.

(2)如果软件运行环境许可,还可以进一步把工作站的硬盘拆除,使之成为一个真正的无盘工作站.只要在工作站的网卡上安装一块远程复位 EPROM 芯片即可.开机后,工作站通过网卡上的这个芯片完成系统引导工作,并直接运行入网程序.这样,工作站既不能从服务器上拷贝文件,也不能向服务器拷贝文件,而只能运行服务器上的文件,杜绝了病毒通过工作站感染服务器的可能性,提高了系统的安全性.

(3)被当做网络服务器使用的机器只专门用来当作服务器,而不再作为工作站使用,也不作为单机使用.

(4)规定只有专业的网络管理人员使用超级用户用户名登录.因为超级用户对于整个网络系统拥有全部权力(包括读、写、建立、删除等),如果工作站上已经感染了病毒,再用超级用户登录,就会感染整个网络服务器.

(5)为用户规定不同的权限,实行专有目录专人使用,防止越权行为,这样即使服务器下的某个用户的子目录感染了病毒,其他的用户如果不执行这个目录下的文件,就不会被病毒感染.

3.2　病毒防火墙

病毒防火墙,实际上是‘广义’防火墙中一个方面的具体实现.它是安装在用户计算机系统之中的反病毒监控软件,它在用户计算机本地系统与外部环境之间完成实时过滤有害病毒的工作,能够有效地阻止来自本地资源和外部网络资源的病毒侵害.

病毒防火墙对病毒的‘过滤’应当具有相当好的实时性,这种实时性表现在一旦病毒入侵系统或者从系统向其它资源感染,病毒防火墙会立刻检测到并加以清除.而传统的单机版反病毒软件则更注重于‘静态’反病毒,即对本地和远程资源以静态分析扫描的方式检测、清除病毒[1].病毒防火墙的‘双向过滤’保证了本地系统不会向远程网络资源传播病毒,这一特点是传统单机版反病毒产品根本无法实现的.

3.3　网络反病毒软件

反病毒解决方案要求包括一套统一全面的实施软件,能够进行中央控制,能对病毒特征码进行自动更新,并且要能支持多平台、多协议和多种文件类型.NAI(美国网络联盟公司)反病毒软件产品占有国际市场超过 60% 的份额,它提供了适合各类企业网络及个人台式机全面的反病毒解决方案 TVD(Toltal Virus Defense).

TVD 包含 3 个套装软件:VSS(VirusScan Security Suite),桌面反病毒解决方案;NSS

(NetShield Security Suite),服务器级反病毒解决方案;ISS(Internet Security Suite),Internet 网关反病毒解决方案.TVD 中所具有的分发控制台(Distribution Console),可以自动接收来自 NAI 的最新病毒特征文件和升级软件.利用这些套装软件,可以建立符合企业需求的病毒防御系统.

3.4 企业级局域网整体病毒防护方案

考虑一个典型的企业级局域网,如图 2 所示.该网由总部局域网和楼外分支机构局域网组成.总部局域网为整个网络系统的中心节点,为应用服务器、电子邮件等业务系统的中心,同时还是网络管理中心,该局域网规模较大,有多种应用,是 Windows NT 与 UNIX 的混合型网络.各分支机构的局域网规模比中心小,中心节点和各分支机构局域网之间通过广域网连接.

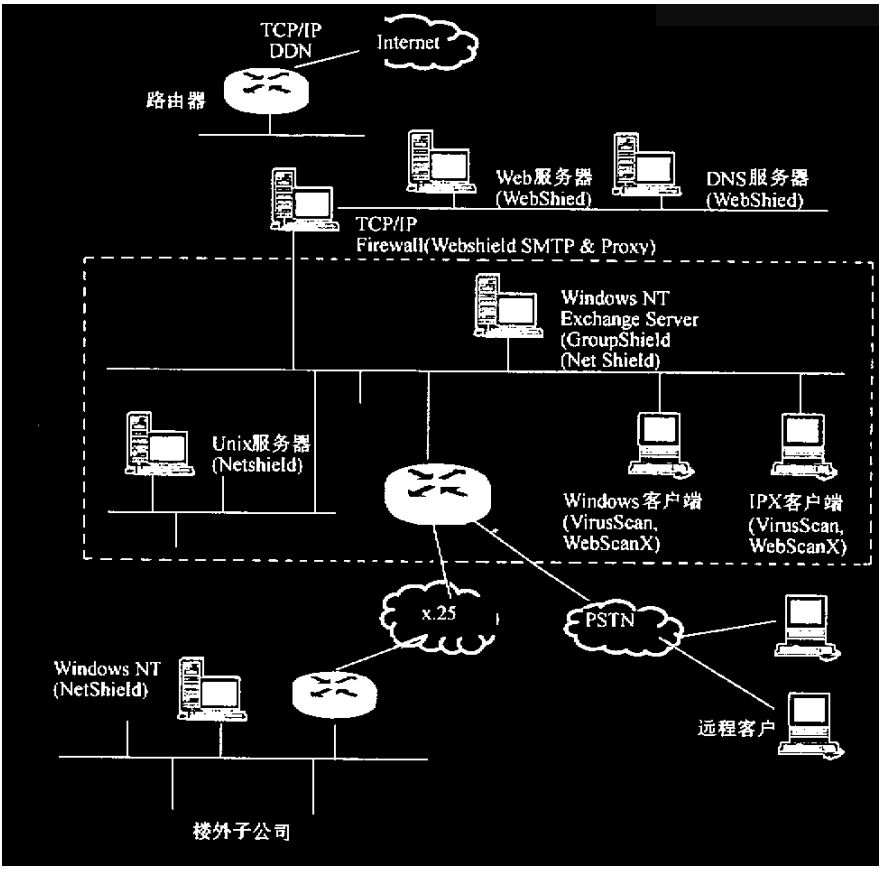

图 2 网络系统整体病毒防护方案结构示意

针对上述典型的企业级局域网,具体布置如下:

(1)客户端反病毒.由于 50%以上的病毒都是通过软盘进入企业网络系统中的,因此对桌面系统的病毒更应该严加防范,此部分可以采用 VSS 产品中的 Virus Scan 进行基于 Windows95/98、Windows 3.x、Windows NT、Mac 和 OS/2 系统的桌面反病毒;采用 WebScanX 以防止用户在下载时,一些恶意 Java 和 ActiveX 小程序对台式机造成破坏;PC Medic 可以对某些系统错误或应用程序运行时出现的错误进行自动修复,以保护系统或应用程序免于崩溃.

(2)服务器反病毒.网络系统的服务器包括 Windows NT、NetWare、Unix 等多种平台.如果服务器被病毒感染,其感染文件必将成为病毒传染的源头,病毒会迅速从桌面感染到整个网络,

直至网络瘫痪. NSS 产品提供了全面的基于服务器的安全保护,可以从单独的直观控制台上远程管理这些服务器平台. 安装 NetShield 进行基于 Windows NT、NetWare 和 Unix 多种平台的服务器反病毒 ;安装 GroupShield 来保护群件服务器.

(3) Internet 反病毒. 据统计,电脑被病毒感染有 20% 是因为从国际互联网下载文件,另外有 26% 是因为电子邮件的附加文件携带病毒. 由于大型网络系统已连入 Internet,因此这一部分也应成为防范的重点. ISS 产品在 Internet 网关上提供全面的病毒防卫系统,封锁病毒所有可能进入点. 通过管理控制台可以直接在服务器或工作站上进行远程管理. 其中包括 :WebShield SMTP 可以扫描全部收发的电子邮件,WebShield Proxy 来扫描 HTTP、FTP 等各种网络协议.

(4)电子邮件反病毒. Lotus Notes,MS Exchange Server,或 Novell 的 Group Wise Server 等是目前比较常用的内部电子邮件系统. Internet 连接采用 SMTP 协议,内部电子邮件系统与 Internet 连接采用 SMTP Gateway. 系统在 Internet 网关处采用 ISS 可以防止从 Internet 上的病毒感染. 内部的电子邮件系统可以在服务器上安装 GroupShield 来扫描 MS Exchange、Lotus Notes/Domino 的病毒以保护群件服务器.

4 小结

随着互联网日益深入到人们的生活、学习、工作当中,防治网络病毒的侵害成为一个重要的课题. 人类和计算机病毒的斗争是个长期的过程,我们需要不断地提高认识,研究和应用新的反病毒技术,以更有效地防治计算机病毒.

[参考文献]

[1] 陈波,于泠. 计算机病毒与反病毒技术的发展[J]. 微机发展,2000,10(6) :79—81.
[2] 胡昌振. 面向 21 世纪网络安全与防护[M]. 北京 :希望电子出版社,1999.

The Solution of Computer Network Virus Defense

Yu Ling,Chen Bo
(College of Mathematics and Computer Science,Nanjing Normal University,Nanjing,210097,PRC)

Abstract :Basic methods of network antivirus in composite environment of different server OS are proposed. We also expatiate upon total virus defense of network. As the example of typical enterprise LAN, the detail virus defense settings are introduced.

Key words :network security ;computer virus ;LAN

[责任编辑 陆炳新]